AMENDMENTS TO CLAIMS

1. (cancelled) A method for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K, the method comprising:

receiving n plaintext blocks, wherein n is an integer greater than 0;

setting Q_0 equal to an initial value; and

for each plaintext block of the n plaintext blocks:

computing $Q_i = E_K(Q_{i-1})$ XOR P_i; and

computing $C_i = M(P_i , Q_i)$,

thereby producing n ciphertext blocks,

wherein:

$0 < i <= n$, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

2. (cancelled) The method according to claim 1 and wherein M is chosen in accordance with a standard indicating bits that are not to be encrypted.

3. (cancelled) The method according to claim 2 and wherein the standard comprises one of the following: an audio standard; a video standard; and an audio-

video standard.

4. (cancelled) The method according to claim 3 and wherein the standard comprises MPEG-2.

5. (cancelled) A method for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K, the method comprising:

receiving n plaintext blocks, wherein n is an integer greater than 0, and an initial value IV;

computing $IV' = M(P_1 , IV)$;

computing $Q_0 = H(IV')$; and

for each plaintext block of the n plaintext blocks:

computing $Q_i = E_K(Q_{i-1})$ XOR P_i ; and

computing $C_i = M(P_i , Q_i)$,

thereby producing n ciphertext blocks,

wherein:

$0 < i <= n$, and

H is a hash function, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M

if bit P_{ij} is to be encrypted.

6. (cancelled) The method according to claim 5 and wherein H comprises SHA1.

7. (cancelled) The method according to claim 5 and wherein H(IV') comprises $E_K(IV')$ XOR IV'.

8. (cancelled) The method according to claim 5 and wherein M is chosen in accordance with a standard indicating bits that are not to be encrypted.

9. (cancelled) The method according to claim 8 and wherein the standard comprises one of the following: an audio standard; a video standard; and an audio-video standard.

10. (cancelled) The method according to claim 9 and wherein the standard comprises MPEG-2.

11. (cancelled) In a method for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K in a stream mode, wherein P_i denotes an i-th plaintext block, and C_i denotes an i-th ciphertext block, an improvement comprising:

for each bit C_{ij} of block C_i , selecting P_{ij} as an output if bit P_{ij} is not to be encrypted.

12. (cancelled) The method according to claim 11 and wherein the stream mode comprises CFM mode.

13. (cancelled) Apparatus for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K, the at least one plaintext block comprising n plaintext blocks, the at least one ciphertext block comprising n ciphertext blocks, wherein n is an integer greater than 0, the apparatus comprising:

an initialization unit for setting Q_0 equal to an initial value; and

a computation unit operative, for each plaintext block of the n plaintext blocks:

to compute $Q_i = E_K(Q_{i-1})$ XOR P_i ; and

to compute $C_i = M(P_i , Q_i)$,

wherein:

$0 < i <= n$, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i , selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

14. (cancelled) Apparatus for producing at least one ciphertext block from at

least one plaintext block using a block cipher E, a key K, and an initial value IV, the at least one plaintext block comprising n plaintext blocks, the at least one ciphertext block comprising n ciphertext blocks, wherein n is an integer greater than 0, the apparatus comprising:

a first computation unit for computing $IV' = M(P_1 , IV)$;

a second computation unit for computing $Q_0 = H(IV')$; and

a third computation unit operative, for each plaintext block of the n plaintext blocks:

to compute $Q_i = E_K(Q_{i-1})$ XOR P_i ; and

to compute $C_i = M(P_i , Q_i)$,

wherein:

$0 < i <= n$, and

H is a hash function, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i , selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

15. (cancelled) In apparatus for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K in a stream mode, wherein P_i denotes an i-th plaintext block, and C_i denotes an i-th ciphertext block, an improvement comprising:

a selector unit operative, for each bit C_{ij} of block C_i , to select P_{ij} as an output if bit P_{ij} is not to be encrypted.

16. (cancelled) A method for producing at least one plaintext block from at least one ciphertext block encrypted using a block cipher E and a key K, the method comprising:

receiving n ciphertext blocks, where n is an integer greater than 0;

setting Q_0 equal to an initial value; and

for each ciphertext block of the n ciphertext blocks:

computing $Q'_i = E_K(Q_{i-1})$ XOR C_i ;

computing $P_i = M(C_i , Q'_i)$; and

computing $Q_i = M(Q'_i , C_i)$,

thereby producing n plaintext blocks,

wherein:

$0 < i <= n$, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i , selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

17. (cancelled) The method according to claim 16 and wherein M is chosen in accordance with a standard indicating bits that are not encrypted

18. (cancelled) The method according to claim 17 and wherein the standard comprises one of the following: an audio standard; a video standard; and an audio-video standard.

19. (cancelled) The method according to claim 18 and wherein the standard comprises MPEG-2.

20. (cancelled) A method for producing at least one plaintext block from at least one ciphertext block using a block cipher E and a key K, the method comprising:

receiving n ciphertext blocks, wherein n is an integer greater than 0, and an initial value IV;

computing $IV' = M(P_1 , IV)$;

computing $Q_0 = H(IV')$; and

for each ciphertext block of the n ciphertext blocks:

computing $Q'_i = E_K(Q_{i-1})$ XOR C_i ;

computing $P_i = M(C_i , Q'_i)$; and

computing $Q_i = M(Q'_i , C_i)$,

thereby producing n plaintext blocks,

wherein:

$0 < i <= n$, and

H is a hash function, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

21. (cancelled) The method according to claim 20 and wherein H comprises SHA1.

22. (cancelled) The method according to claim 20 and wherein H(IV') comprises E_K(IV') XOR IV'.

23. (cancelled) The method according to claim 20 and wherein M is chosen in accordance with a standard indicating bits that are not encrypted.

24. (cancelled) The method according to claim 23 and wherein the standard comprises one of the following: an audio standard; a video standard; and an audio-video standard.

25. (cancelled) The method according to claim 24 and wherein the standard comprises MPEG-2.

26. (cancelled) In a method for producing at least one plaintext block from at least one ciphertext block using a block cipher E and a key K in a stream mode, wherein P_i denotes an i-th plaintext block of the plurality of plaintext blocks, and

C_i denotes an i-th ciphertext block of the plurality of ciphertext blocks, an improvement comprising:

for each bit P_{ij} of block P_i , selecting C_{ij} as an output if bit C_{ij} is not encrypted.

27. (cancelled) The method according to claim 26 and wherein the stream mode comprises CFM mode.

28. (cancelled) Apparatus for producing at least one plaintext block from at least one ciphertext block encrypted using a block cipher E and a key K, the at least one ciphertext block comprising n ciphertext blocks, the at least one plaintext block comprising n plaintext blocks, wherein n is an integer greater than 0, the apparatus comprising:

initialization apparatus for setting Q_0 equal to an initial value; and

a computation unit operative, for each ciphertext block of the n ciphertext blocks:

to compute $Q'_i = E_K(Q_{i-1})$ XOR C_i ;

to compute $P_i = M(C_i , Q'_i)$; and

to compute $Q_i = M(Q'_i , C_i)$,

wherein:

$0 < i <= n$, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i , selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

29. (cancelled) Apparatus for producing at least one plaintext block from at least one ciphertext block using a block cipher E and a key K, the at least one ciphertext block comprising n ciphertext blocks, the at least one plaintext block comprising n plaintext blocks, wherein n is an integer greater than 0, the apparatus comprising:

a first computation unit for computing $IV' = M(P_1 , IV)$;

a second computation unit for computing $Q_0 = H(IV')$; and

a third computation unit operative, for each ciphertext block of the n ciphertext blocks:

to compute $Q'_i = E_K(Q_{i-1})$ XOR C_i ;

to compute $P_i = M(C_i , Q'_i)$; and

to compute $Q_i = M(Q'_i , C_i)$,

wherein:

$0 < i <= n$, and

H is a hash function, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i , selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit

P_{ij} is encrypted.

30. (cancelled) In apparatus for producing at least one plaintext block from at least one ciphertext block using a block cipher E and a key K in a stream mode, wherein P_i denotes an i-th plaintext block of the plurality of plaintext blocks, and C_i denotes an i-th ciphertext block of the plurality of ciphertext blocks, an improvement comprising:

a selector unit operative, for each bit P_{ij} of block P_i , to select C_{ij} as an output if bit C_{ij} is not encrypted.

31. (Currently Amended) A system for ~~scrambling/~~descrambling at least one packets~~,~~ the at least one packet having a must stay clear (MSC) section which must always stay in the clear, the system comprising a ~~scrambling/~~descrambling device to:

compute a Cipher Initialization Vector for the at least one packet as a function of at least part of the MSC section of the at least one packet; and

~~scramble/~~descramble the at least one packets so that the at least one packet is descrambled ~~based on~~using ~~an~~ the Cipher Initialization Vector~~alue~~ of the at least one packet and a Key as input~~, each of the packets having a must stay clear (MSC) section which must always stay in the clear, the Initial Value for each of the packets being a function of at least part of the MSC section of an associated one of the packets being processed~~.

32. (Currently Amended) The system according to claim 31, wherein the MSC section includes an adaptation field, the Cipher Initialization Vector~~alue~~ of the at least one packet being computed as a function of at least part of the adaptation field of the at least one packet ~~being processed~~.

33. (Currently Amended) The system according to claim 32, wherein the Cipher Initialization Vector~~alue~~ of the at least one packet is a function of the data content of the adaptation field of the one packet ~~being processed~~.

34. (Currently Amended) A method for ~~scrambling/~~descrambling at least one packets, ~~each of~~ the at least one packets having a must stay clear (MSC) section which must always stay in the clear, the method comprising:

~~determining~~ computing an Cipher Initialization Vector~~alue~~ for ~~each of~~ the at least one packets as a function of at least part of the MSC section of ~~an associated~~the at least one ~~of the~~ packets ~~being processed~~; and

~~scrambling/~~descrambling the at least one packets so that the at least one packet is descrambled ~~based on~~using the Cipher Initialization Vector~~alue~~ of the at least one packet and a Key as input.

35. (Currently Amended) The method according to claim 34, wherein the MSC section includes an adaptation field, the ~~determining~~ computing ~~including determiningof~~ the Cipher Initialization Vector~~alue~~ of the at least one packet being performed as a function of at least part of the adaptation field of the at least one packet ~~being processed~~.

36. (Currently Amended) The method according to claim 35, wherein the ~~determining~~ computing ~~includes determiningof~~ the Cipher Initialization Vector~~alue~~ of the at least one packet is performed as a function of the data content of the adaptation field of the at least one packet ~~being processed~~.

37. (cancelled) Apparatus for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K, the at least one plaintext block comprising n plaintext blocks, the at least one ciphertext block comprising n ciphertext blocks, wherein n is an integer greater than 0, the apparatus comprising:

means for setting Q_0 equal to an initial value; and

means for computing:

$Q_i = E_K(Q_{i-1})$ XOR P_i ; and

$C_i = M(P_i , Q_i)$, for each plaintext block of the n plaintext blocks,

wherein:

$0 < i <= n$, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

38. (cancelled) Apparatus for producing at least one ciphertext block from at least one plaintext block using a block cipher E, a key K, and an initial value IV, the at least one plaintext block comprising n plaintext blocks, the at least one ciphertext block comprising n ciphertext blocks, wherein n is an integer greater than 0, the apparatus comprising:

means for computing $IV' = M(P_1 , IV)$;

means for computing $Q_0 = H(IV')$; and

means for computing:

$Q_i = E_K(Q_{i-1})$ XOR P_i ; and

$C_i = M(P_i , Q_i)$, for each plaintext block of the n plaintext blocks,

wherein:

$0 < i <= n$, and

H is a hash function, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

39. (cancelled) Apparatus for producing at least one plaintext block from at least one ciphertext block encrypted using a block cipher E and a key K, the at least one ciphertext block comprising n ciphertext blocks, the at least one plaintext block comprising n plaintext blocks, wherein n is an integer greater than 0, the apparatus comprising:

means for setting Q_0 equal to an initial value; and

means for computing:

$Q'_i = E_K(Q_{i-1})$ XOR C_i ;

$P_i = M(C_i , Q'_i)$; and

$Q_i = M(Q'_i , C_i)$, for each ciphertext block of the n ciphertext blocks,

wherein:

$0 < i <= n$, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

40. (cancelled) Apparatus for producing at least one plaintext block from at least one ciphertext block using a block cipher E and a key K, the at least one ciphertext block comprising n ciphertext blocks, the at least one plaintext block comprising n plaintext blocks, wherein n is an integer greater than 0, the apparatus comprising:

means for computing $IV' = M(P_1 , IV)$;

means for computing $Q_0 = H(IV')$; and

means for computing:

$Q'_i = E_K(Q_{i-1})$ XOR C_i;

$P_i = M(C_i , Q'_i)$; and

$Q_i = M(Q'_i , C_i)$, for each ciphertext block of the n ciphertext blocks,

wherein:

$0 < i <= n$, and

H is a hash function, and

P_i denotes an i-th plaintext block of the n plaintext blocks, and

C_i denotes an i-th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

41-42. (cancelled)

43. (New) A system for scrambling at least one packet, the at least one packet having a must stay clear (MSC) section which must always stay in the clear, the system comprising a scrambling device to:

compute a Cipher Initialization Vector for the at least one packet as a function of at least part of the MSC section of the at least one packet; and

scramble the at least one packets so that the at least one packet is scrambled using the Cipher Initialization Vector of the at least one packet and a Key as input.

44. (New) The system according to claim 43, wherein the MSC section includes an adaptation field, the Cipher Initialization Vector of the at least one packet being computed as a function of at least part of the adaptation field of the at least one packet.

45. (New) The system according to claim 44, wherein the Cipher Initialization Vector of the at least one packet is a function of the data content of the adaptation field of the one packet.

46. (New) A method for scrambling at least one packet, the at least one packet having a must stay clear (MSC) section which must always stay in the clear, the method comprising:

computing a Cipher Initialization Vector for the at least one packets as a function of at least part of the MSC section of the at least one packet; and

scrambling the at least one packets so that the at least one packet is scrambled using the Cipher Initialization Vector of the at least one packet and a Key as input.

47. (New) The method according to claim 46, wherein the MSC section includes an adaptation field, the computing of the Cipher Initialization Vector of the at least one packet being performed as a function of at least part of the adaptation field of the at least one packet.

48. (New) The method according to claim 47, wherein the computing of the Cipher Initialization Vector of the at least one packet is performed as a function of the data content of the adaptation field of the at least one packet.